Remarks

<u>Status of application</u>

Claims 1-99 were examined and stand rejected in view of prior art. The Examiner's courtesy of a telephone interview on December 4, 2009 is appreciated. Further to that telephone interview, the claims have been amended to provide clarification of Applicant's invention. Reexamination and reconsideration are respectfully requested.

<u>The invention</u>

Please refer to Applicant's prior filed responses (e.g., Amendment filed September 15, 2008) for a concise summary of Applicant's invention.

<u>Prior art rejections</u>

A. Section 102(e): He

Claims 1-31, 36-65, 70-73, and 78-99 stand rejected under 35 U.S.C. 102(e) as being unpatentable over He et al. (US Patent 7,269,729 B2, hereafter "He"). Applicant's claimed invention is fundamentally different and thus can be distinguished.

As discussed during the telephone interview, Applicant's approach is very unique: the whole process of dealing with column encryption keys can be handled by the user entirely within SQL statements that the user provides to the database system. For example, all tasks related to creating and using an encryption key can be carried out under user direction entirely within SQL, using the SQL extensions provided by Applicant's invention. There is no need for the user to "drop out" of the database system to launch a separate program for this purpose. The same holds true for key management, including for instance altering keys or dropping keys. Such an approach stands in stark contrast to He's approach, which requires encryption keys to have been previously set up -- He explicitly indicates that his system does <u>not</u> provide any such capability (see, e.g., He at Col. 6, lines 42-60).

The advantages of Applicant's approach are numerous. For purposes of brevity, these advantages will not be repeated in this document, but can easily be found detailed in Applicant's previous responses (see, e.g., p. 18 of Applicant's Request for

Reconsideration filed March 9, 2009). Simply put, Applicant's approach allows the database user to control all aspects of a column encryption key (e.g., creation, management, and usage) thru SQL without involving components outside the DBMS. It is Applicant's understanding that the Examiner appreciates this difference, and agrees that Applicant's invention can be distinguished from He. Therefore, the task at hand is to clarify the claim language to capture these distinctive features (to the satisfaction of the Office). To that end and in consultation with the Examiner, Applicant's claims are amended herein to bring such distinguishing features to the forefront.

For example, claim 1 has been amended to recite more precisely that creation of the encryption key is carried out through a SQL statement utilizing Applicant's SQL extensions. Significantly, the SQL extensions are used to specify creation of a "named encryption key" for encrypting column data, where the named encryption key is identified in the SQL statement by a user-assigned syntactically unique name:

> receiving a first SQL statement that uses said SQL extensions to
> specify creation of a named encryption key for encrypting column data,
> said named encryption key being identified in said first SQL statement by
> a user-assigned syntactically unique name;

(Applicant's other independent claims have been amended in a like manner.) This claim language stands in stark contrast to He's teaching, which expressly states that the encryption keys are previously set up outside of the database (and certainly outside of SQL) in a separate directory server.

The significance of the "named" (i.e., user-assigned syntactically unique name) encryption key is made apparent by subsequent claim language. For example, amended claim 1 recites that a subsequent SQL statement is issued that uses the SQL extensions to specify creation of a database table having particular column data encrypted with the named encryption key, such that the named encryption key is identified in the SQL statement by the user-assigned syntactically unique name:

> receiving a second SQL statement that uses said SQL extensions to

19

> specify creation of a database table having particular column data encrypted with said named encryption key, said named encryption key being identified in said second SQL statement by said user-assigned syntactically unique name;

Again, this stands in stark contrast to He's approach. At Col. 7, Line 42, He states that the user "explicitly supplies her private key." In particular, He's reference ("SK_A") to a key in a SQL statement is not some sort of "named key." Instead, as He expressly states, SK_A is shorthand to indicate that the user "explicitly supplies her private key."

For the reasons stated, it is respectfully submitted that Applicant's named encryption key approach is not shown in the prior art and thus represents a patentable advance in the area of database encryption and security. Particularly in view of clarifying amendments made herein, it is believed that the claims are patentable and any rejection under Section 102 is overcome.

B. Section 103: He and Newman

Claims 32-35, 66-69, and 74-77 stand rejected under 35 U.S.C. 103(a) as being anticipated by He et al. (US Patent 7,269,729 B2) in view of Newman et al. US Patent 7,266,699 B2). Here, the Examiner repeats the rejection based on He, but adds Newman for the proposition that it teaches the claim limitation pertaining to a named encryption key itself being encrypted from a user-supplied password. The claims are believed to be allowable for at least the reasons stated above pertaining to the Section 102 rejection based on He. In particular, the combination of He and Newman fails to teach Applicant's approach of using SQL extensions that allow the tasks of creating, maintaining, and using encryption keys to be performed entirely within the confines of SQL statements written by database users. Newman contains no disclosure that remedies this core deficiency of He.

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: December 10, 2009 /John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX